Eine Einführung in

Internet Firewalls

von

Roland LIEGER

Harput VAHAN

Grzegorz RUMATOWSKI

Patrick AWART

Inhalt:

1. Einleitung:

In den letzten Jahren hat sich das Internet von einem unbekannten Werkzeug für Militär und Wissenschaft zu einem Medium für verwandelt, daß für jeden technisch Interessierten verfügbar ist. Es ist anzunehmen, daß, getrieben durch WWW (World Wide Web) und den Mythos der unbeschränkten Verfügbarkeit von Information, das Netz der Netze auch in den nächsten Jahren weiter an Bedeutung gewinnen wird und immer weitere Kreise der Bevölkerung elektronisch miteinander kommunizieren werden. Gleichzeitig entsteht elektronischer Handel und führt damit zu einer Kommerzialisierung des Netzes. Sowohl der größere Benutzerkreis als auch die höhere wirtschaftliche Bedeutung der versandten Nachrichten führt zu vermehrter Sorge um die Sicherheit im Netz. Bevor man daran geht, Schutzmechanismen zu erarbeiten, sollte man sich stets vor Augen führen, was man eigentlich wovor schützen will. Im Bereich der Datennetze sind dies wohl vor allem:

- **Daten** - Dabei geht es sowohl darum daß Daten nicht Unbefugten bekannt werden (Vertraulichkeit/Datendiebstahl), als auch darum daß, legitime Benutzer stets Zugriff haben (Verfügbarkeit) und sicher sein können, daß die Daten nicht von Dritten verfälscht wurden (Integrität).
- **EDV-Resourcen** - Wer für einen Computer bezahlt möchte im allgemeinen auch darüber

bestimmen für welche Zwecke er eingesetzt wird. Auch wenn viele Computer über ungenutzte Resourcen (CPU-Zeit, Plattenplatz) verfügen, so kann es doch sein, daß man diese eines Tages benötigt, und dann ist es schwer den vorher unfreiwillig überlassenen Platz wieder zurück zu erobern. Weiters muß verhindert werden, daß Außenstehende das Rechnersystem lahmlegen, sei es indem sie ihn vorsätzlich zum Absturz bringen (Denial of Service Attack) oder indem sie so viele Jobs starten, daß für andere Benutzer keine Kapazität mehr übrigbleibt.
- **Reputation** - Wenn Unbefugte Zugriff auf einen Computer haben, ist es ihnen ein Leichtes im Namen der legitimen Benutzer Daten (per EMail oder FTP) zu verbreiten, die gegen die guten Sitten und/oder Gesetze verstoßen (etwa Raubkopien, Pornographie, Rassistische Schriften). Da es für die legitimen Benutzer kaum möglich ist nachzuweisen, daß sie diese Daten nicht gesendet haben, kann ihr Ansehen so schwer geschädigt werden.

Weiters stellt sich die Frage, vor wem man die Rechner schützen möchte. Mögliche Angreifern sind:

- **Spaßvögel** - Machen sich ein Vergnügen daraus in fremden Datenbeständen ohne konkretes Ziel herumzustöbern. Sie sind im Grunde harmlos und beschädigen im allgemeinen nichts es sei denn durch Ungeschick beim Versuch ihre Spuren zu verbergen.
- **Punktesammler** - Die Motivation des Punktesammlers besteht darin möglichst viele (nach Möglichkeit schnelle, exotische oder prominente) Computer zu knacken. Die Freude besteht im Überwinden der Sicherheitsmechanismen. Wie die Spaßvögel sind sie im Grunde harmlos, doch geben sie ihr Know-How oft an andere weniger Wohlgesonnene weiter.
- **Vandalen** - Ihr Ziel ist maximale Zerstörung. Durch ihr rücksichtloses Vorgehen werden Vandalen stets rasch bemerkt, doch der Schaden, den sie bis dahin angerichtet haben kann schon groß sein. Vandalen sind vor allem dann ein Problem, wenn das Netzwerk von einem großen, bekannten Unternehmen mit unzufriedene Kunden betrieben wird.
- **Spione** (aus Industrie/Geheimdienst/Militär) - Viele geheime Daten lassen sich gut an Konkurrenten verkaufen. Ein Spion wird nur selten irgendetwas in dem besuchten Netzwerk verändern und ist daher nur sehr schwer zu fangen. Vorsicht: Daten lassen sich nicht nur über Datenleitungen transportieren. Man sollte nie übersehen, daß auch die Möglichkeit Daten auf Disketten oder Magnetbändern zu transportieren unterbunden werden muß.
- **Dummheit/Unfälle** (Schiebe nicht auf Bosheit, was auch durch Dummheit gut erklärt werden kann!) - Auch legitime Benutzer handeln nicht immer optimal.

Sicherheitsmodelle:

Nachdem man die verschiedenen Arten von Gefahren betrachtet hat, kann man sich nun ein Sicherheitsmodell überlegen. Übliche Ansätze sind etwa:

- **Keine Sicherheit** - Man ignoriert die Gefahr. Das hat zwar den Vorteil, daß kurzfristig kein Aufwand anfällt, wenn aber doch Probleme auftreten werden sie wohl erst sehr spät bemerkt, und sind dann schwer zu beheben.
- **Sicherheit durch Täuschung** (Security by Obscurity) - Angreifer werden durch gezielte Desinformation getäuscht. Etwa meldet der Begrüßungsprompt das falsche Betriebssystem, Dateien sind 'kreativ' benannt und stehen an seltsamen Plätzen im Verzeichnisbaum. Auch der Rechnername kann unübliche Zeichen enthalten, und wird natürlich nicht bekanntgemacht. Das Problem dieses Ansatzes ist, daß einerseits auch die legitimen Benutzer leicht getäuscht werden und andererseits intelligente Programme existieren, die schnell Übersicht in das Chaos bringen. Somit bietet auch gute Täuschung keine echte Sicherheit.
- **Rechnerzentrierte Sicherheit** - Jeder Rechner wird für sich geschützt. Dazu werden etwa die üblicherweise unter UNIX verfügbaren Mechanismen zur Benutzer- und Gruppenverwaltung verwendet, sowie Rechte an Resourcen an bestimmte Nutzer vergeben (etwa Lese- und Schreibrechte für bestimmte Dateien und Verzeichnisse, Nutzungsrechte für Programme, Diskquota, Druckerquota). Auch wenn alle realen Implementationen in dem einen oder

anderen Bereich Schwächen aufweisen, so biete dieses Verfahren gute Sicherheit, wenn es konsequent angewendet wird. Das zentrale Problem rechnerzentrierter Sicherheit besteht darin, daß jeder (!) Rechner einzeln geschützt werden muß. Da in einem größeren Netz nie zu verhindern ist, daß irgendwo ein neuer Rechner angeschafft und aufgestellt wird, oder ein neues Programm auf einem bestehenden Rechner installiert wird, ohne daß die Sicherheitsverantwortlichen darüber informiert sind, können leicht Lücken in der Verteidigung entstehen. Diese Lücken sind zwar zwischen sicheren Rechnern versteckt, doch ist das wieder nur Sicherheit durch Täuschung.

- **Netzwerkzentrierte Sicherheit** - Es wird ein ganzes Netzwerk aus vielen Rechnern gemeinsam geschützt. Dabei wird davon ausgegangen, daß alle Rechner des Netzes relative sicher sind, und die Gefahr vor allem von außen (externen Netzen) kommt. Diese Methode zur Sicherung kann durch eine Firewall realisiert werden. Wir werden uns im weiteren auf Firewalls konzentrieren, auch wenn dies sicher nicht die einzige Möglichkeit ist.

Bei der obigen Aufzählung von Sicherheitsmodellen man allerdings bedenken, daß es keine Lösung gibt, die alle Probleme abdeckt. In der Praxis wird man daher stets eine Kombination mehrerer Systeme wählen (im allgemeinen Netzwerk- und Rechnerzentrierte Sicherheit).

Firewalls

Eine Firewall dient dazu, ein internes Netzwerk mit einem öffentlichen Netzwerk zu verbinden, von dem man annehmen muß, daß es potentielle Angreifer beherbergt. Dabei sollen den internen Nutzern die Vorteile des Internets zugänglich gemacht werden, ohne dabei Unbefugten Zugriff auf interne Daten zu bieten.

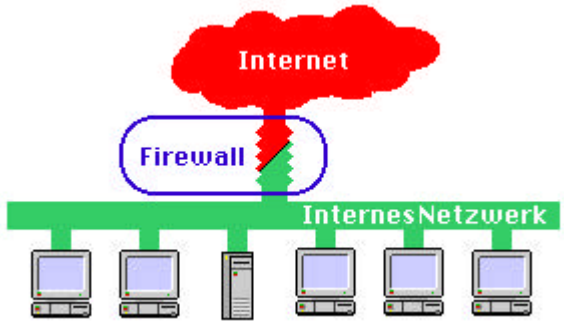

Fig1.: Eine Firewall als Grenze zwischen Internet und internem Netzwerk

Welche Sicherheit bietet eine Firewall?

Was eine Firewall leistet:

- **Fokus für Sicherheitsentscheidungen** - Die Installation einer Firewall macht es nötig klare Richtlinien für die Sicherheit in einem Computernetzwerk zu definieren. Damit wird vermieden, daß nur ein unscharfer Sicherheitsbegriff besteht, der dazu führt, daß bei konkreten Problemen stets ad-hoc Entscheidungen getroffen werden, die dann leicht untereinander inkonsistent sind.
- **Zentraler Verbindungsknoten** - Alle Daten die zwischen internem und externem Netz ausgetauscht werden, müssen durch die Firewall. Damit ist es möglich in der Firewall die Durchsetzung der Sicherheitspolitik zu erzwingen, bzw. Verstöße gegen Sicherheitsrichtlinien zu erkennen und zu protokollieren.
- **Begrenzung der Angriffsfläche** - Ein externer Angreifer muß zunächst die Firewall überwinden, bevor er einen der internen Rechner attackieren kann. Da die Firewall eine (im Verhältnis zu einem großen, internen Netzwerk) kleine und daher überschaubare Einheit darstellt, ist eine gute Verteidigung der Firewall relativ einfach und erfolgversprechend. Das

bedeutet natürlich nicht, daß man völlig auf eine rechnergestützte Verteidigung im internen Netz verzichten kann, aber ein Angreifer sollte stets von der Firewall abgefangen werden und keine Möglichkeit haben, die Stärken und Schwächen der internen Verteidigung zu erforschen.

Wovor eine Firewall KEINEN Schutz bietet:

- **Angriffen durch Insider** - Eine Firewall schützt die Rechner des internen Netzes vor Angriffen von Außen. Sie schützt nicht vor Angriffen die innerhalb des lokalen Netzes vor sich gehen (etwa durch Personen, die (legitim oder auch nicht) physischen Zugang zu dem angegriffenen Computer haben).
- **Umgehung durch weitere Datenleitungen** - Eine Firewall kann nur jene Datenpakete untersuchen, die durch sie geschickt werden. Wenn neben der offiziellen, durch die Firewall überwachten, Verbindung noch andere existieren (etwa privat installierte Modems innerhalb des internen Netzes) so kann die Firewall natürlich nicht überprüfen welche Daten dort über die Leitung wandern. Insbesondere besteht dann die Gefahr, daß die Firewall von innen heraus angegriffen wird, und so über die Hintertür der Hauptzugang geöffnet wird.
- **Viren, Trojanische Pferde & Co.** - Eine Firewall verfügt über kein Verständnis für den Inhalt der Daten die durch sie fließen. Es gibt zu viele Protokolle, Kompressionsverfahren und Computertypen um automatisch sicher zu erkennen wann ein Datenpaket Teil eines Programms ist um dann einen Virenscanner zu starten.
- **Unbekannte Gefahren** - Jede Aufzählung aller möglichen Gefahrenquellen ist am Tag ihrer Erstellung veraltet. Es werden stets neue Fehler in bekannten Programmen gefunden und neue Sicherheitslücken aufgedeckt. Keine einmal geschaffene Lösung kann alle zukünfig gefundenen Probleme vorausahnen und lösen.

---

2. Internet Dienste

In Computernetzwerken wird eine Vielzahl verschiedener Dienste (und damit verbundener Protokolle) eingesetzt. Jeder davon bringt seine speziellen Nutzen aber auch spezifische Sicherheitsprobleme. Einige der wichtigsten und verbreitesten Protokolle soll im folgenden kurz besprochen werden. Eine detailierte Beschreibung zur optimalen Konfiguration aller Dienst folgt in Kapitel 9.

- **Elektronische Post** (Electronic Mail) - EMail ist der wohl der bekannteste und am meisten genutzte Dienst im Internet. Die Probleme die sich aus der Nutzung von EMail ergeben stammen aus mehreren Richtungen. Einerseits ist sendmail, das sind in UNIX Systemen um die Verwaltung von EMails kümmert, bekannt für seine Sicherheitslücken, die zwar immer wieder geflickt werden, doch werden fast genauso schnell neue Bugs gefunden. Andererseits besteht die Gefahr, daß Benutzer Anweisungen, die sie über EMail erhalten (etwa: Bitte das Passwort sofort auf xyz ändern) unreflektiert befolgen wenn sich der Absender als Administrator ausgibt, und so Sicherheitslücken schaffen. Weiters besteht die Gefahr daß Benutzer unbewußt oder vorsätzlich Massenmails aussenden und so das Netz überfluten. Zuletzt sei auch noch erwähnt, daß es auch möglich ist Programme über EMail zu versenden. Damit besteht auch die Möglichkeit Viren und Trojanische Pferde über EMail einzuschleppen.
- **File Transfer Protocol** - FTP ist das wichtigste Protokoll wenn es darum geht Programme zu übertragen. Damit besteht natürlich die Gefahr, daß Viren oder Trojanische Pferde eingeschleppt werden. Viel wahrscheinlicher ist es allerdings daß mit unkontrolliertem FTP (intakte) Programme eingeschleppt werden, die aus Sicht des Netzwerkbetreibers unerwünscht sind (etwa Spiele, die während der Arbeitszeit die Mitarbeiter von der Arbeit abhalten oder raubkopierte Software, Pornos etc.). Umgekehrt besteht die Gefahr, daß Benutzer per

(anonymous) FTP Daten (wissentlich oder unerwartet) für die Allgemeinheit zur Verfügung stellen die nicht für jedermann bestimmt sind. Ein weiteres Problem von FTP sind von jedermannbeschreibbare Filesysteme. Hier kann es vorkommen, daß Hacker den Plattenplatz zum geheimen Datenaustausch verwenden, indem einer die Daten per FTP aufspielt und ein anderer sie später von dort wieder abholt. Obwohl dies kein unmittelbares Sicherheitsrisiko ist, besteht doch das Problem, daß der Computerbetreiber zum unfreiwilligen Helfer krimineller Aktionen wird, und daß weiters Plattenplatz für Zwecke genutzt wird für die er nicht bestimmt war.

- **Remote Login** - Telnet (das wohl wichtigste Protokoll für Remote Login) galt lange Zeit als sicherer Dienst, da es erfordert, daß sich der Benutzer beim Computer identifiziert. Erst in letzter Zeit ist das Abhören der Passwörter bei der Login-Prozedur zum Problem geworden. Ein möglicher Ausweg aus diesem Problem ist die Verwendung von Einweg-Passwörtern. Anders ist die Situation bei rsh bzw. rlogin. Diese Dienste beruhen auf einem Vertrauen der Rechner untereinander und sind daher in nicht vertrauenswürdigen Netzen vollkommen unsicher.
- **Usenet News** - News ist ein sehr sicheres Protokoll. Das zentrale Problem besteht in dem enormen Datenvolumen, das schnell zur Erschöpfung des verfügbaren Plattenplatzes führen kann.
- **Domain Name Service** - DNS ermöglicht eine Abbildung von Rechnernamen auf IP-Adressen. Auch wenn dieser Dienst kaum direkt von Menschen genutzt wird, so bildet er doch eine Grundlage für fast alle anderen Netzdienste. Damit bildet er auch eine zentrale Schwachstelle aller Netzdienste. Wenn DNS unterlaufen wird, so werden IP-Pakete (mit möglicherweise sensiblem Inhalt) an die falschen Rechner gesandt. Daher sollte der DNS-Server für das interne Netzwerk stets im Netzwerk enthalten (und damit geschützt) sein, und Meldungen externer DNS-Server nur mit Vorsicht verwendet werden.
- **Internet Control Message Protocol** - Das ICMP einzelne Rechner und insbesondere Router über den Zustand der Leitungen (up/down, relative Last) zu informieren, so daß diese geschickte Routineentscheidungen fällen können. Wenn diese Meldungen stets beherzigt werden, kann es passieren, daß interne Meldungen plötzlich über externe Knoten geroutet werden, weil diese (fälschlicherweise) vorgegaukelt haben, daß sie über gute Verbindungen zum eigentlichen Zielrechner verfügen.
- Es gibt noch andere praktisch wichtige Netzdienste (etwa HTTP, NFS, Time Service, X Windows, Print Server) die alle ihre speziellen Nutzen und Sicherheitsrisken haben. Aus Platzgründen (und da jede noch so komplette Aufzählung immer noch lückenhaft wäre) sollen sie hier nicht besprochen werden.

Für jede Dienst den ein Netzwerk leisten kann muß man sich überlegen, wie der zu erwartende Nutzen in Relation zu den möglichen Gefahren liegt und dann entscheiden ob man ihn über die Firewall hinweg erlauben will oder ihn lieber verbietet.

---

3. Sicherheits-Strategien:

Bevor nun einzelne Details im Aufbau von Firewalls besprochen werden, sollen noch einige Grundlegende Prinzipien jeder geschickten Sicherheitsstrategie erwähnt werden:

- **Minimale Privilegien** - Jeder Knoten und Benutzer im Netzwerk bekommt nur genau jene Rechte, die er zur Erfüllung seiner Aufgabe unbedingt benötigt und nicht mehr (aber auch nicht weniger, sonst werden Mechanismen zur Umgehung gesucht (und gefunden)).
- **Mehrstufige Verteidigung** - Wenn einer Verteidigungslinie durch einen Angreifer überwunden wird, so soll er damit nicht uneingeschränkte Gewalt über das System haben, sondern zunächst vor einer weiteren Verteidigungslinie stehen. Natürlich läßt sich dieses

System nicht auf unbegrenzt viele Ebenen ausdehnen, doch jede zusätzlich Linie kostet den Angreifer Zeit, und gibt dem Systemadministrator die Chance etwas gegen die Attacke zu unternehmen.
- **Zentraler Verbindungsknoten** mit Drosselfunktion - Dadurch daß aller Verkehr durch *einen* Knoten muß, ist es möglich diesen genau zu Überwachen und ggf. Verbindungen die auf einen Angriff hindeuten zu unterbinden. Es ist viel einfacher einen (auch großen) Knoten zu überwachen als eine Vielzahl kleiner Verbindungen.
- **Schwächstes Glied** - Jede Kette ist nur so stark wie ihr schwächstes Glied. Ein Angreifer wird immer den am wenigsten verteidigten Punkt suchen und dort angreifen. Es macht also beispielsweise wenig Sinn EMails scharf zu überprüfen, aber FTP freizugeben.
- **Ausfallsicher** - Jedes noch zu gute Sicherheitssystem hat seine Schwächen. Es ist niemals möglich im vorhinein an alle möglichen Sonderfälle zu denken und diese mit Regeln abzudecken. Daher ist es nötig sich zu überlegen, was in unbekannten Situationen zu tun ist. Dazu bieten sich primär zwei Philosophien an:
    - Alles was nicht explizit verboten ist, ist erlaubt. - Erst wenn ein Dienst als zu gefährlich im Verhältnis zu seinem Nutzen erkannt wird, wird er verboten. Der Nachteil dieses Ansatzes besteht darin, daß eine Entscheidung immer erst dann getroffen wird, wenn bereits ein Schaden eingetreten ist. Es ist sogar möglich, daß ein Angreifer bewußt ein auffälliges Problem erzeugt, das die Aufmerksamkeit des Systemadministrators beansprucht um im entstehenden Chaos unbemerkt eine echte Attacke starten zu können.
    - Alles was nicht explizit erlaubt ist, ist verboten. - Hier ist von vorne herein alles verboten und somit maximale Sicherheit gegeben. Erst wenn ein Dienst auf das Verhältnis von Nutzen zur Sicherheitsrisiko überprüft wurde wird er freigegeben. Damit ist die Nutzung neuartiger Dienste zwar etwas schwerfälliger, doch werden auch alle neuen Gefahren automatisch abgeschirmt. Aus Sicht der Systemsicherheit ist diese Philosophie der liberaleren Ersten weit überlegen.
- **Diversitäre Systeme** - Wenn alle Komponenten eines Sicherheitssystems aus einer Hand stammen, besteht stets die Gefahr, daß alle die gleiche Schwachstelle enthalten, und bei einem Angriff gemeinsam überwunden werden können. Je unterschiedlicher die Systeme, desto unwahrscheinlicher sind gemeinsame Fehler (desto komplizierter, weil uneinheitlicher, aber auch die Installation und Wartung).
- **Mitarbeit aller Betroffenen** - Es ist unbedingt erforderlich bei allen Benutzer des Netzwerkes Verständnis für die Notwendigkeit der gewählten Sicherheitsmaßnahmen zu erzeugen und sie (mehr oder minder) freiwillig zur Mitarbeit an der Systemsicherheit zu gewinnen. Menschen, die das Gefühl haben, daß ihnen eine Maßnahme (deren Sinn sie nicht verstehen) gegen ihren Willen aufgezwungen wird, entwickeln eine erstaunliche Kreativität und Einsatzfreude wenn es darum geht, die unbeliebte Maßnahme zu umgehen.
- **Einfachheit** - Je simpler ein System ist, desto weniger Möglichkeiten gibt es Fehler zu machen und desto weniger Kosten entstehen dafür diese Fehler zu beheben.

---

4. Grundtypen von Firewalls:

Bei der Konstruktion einer Firewall muß man entscheiden, auf welcher Ebene man erlaubten von verbotenem Datenverkehr trennen will. Dabei stehen im wesentlichen zwei Möglichkeiten offen:

- **IP-Paket Filter** - Für jedes IP-Paket wird allein auf Basis der in ihm enthaltenen Information (Source und Destination IP-Adresse, Portnummer, Status-Bits, aber ohne daß Statusinformation gesammelt und ausgewertet wird) entschieden ob es durch die Firewall darf oder nicht. Die meisten kommerziellen Router können mit (mehr oder minder komplexen) Regeln zur Filterung von IP-Paketen programmiert werden, doch ist zu beachten, daß viele

Implementierungen nicht intuitiv zu verwenden (und daher fehleranfällig in der Verwendung), oder selbst fehlerhaft sind.

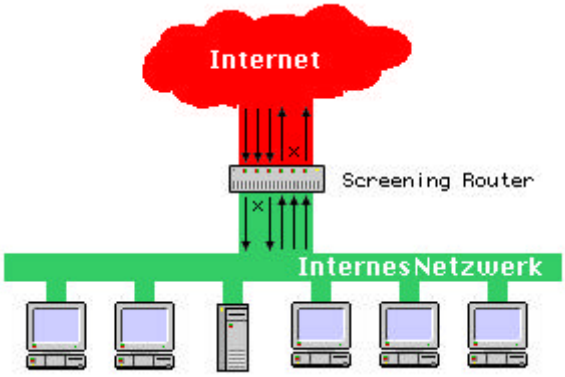

Fig.2: Ein Router zwischen internem Netz und dem Internet filtert IP-Pakete.

- **Proxy Systeme** filtern den Datenstrom auf Applikationsebene (Application Level Gateway). Sie nehmen dazu eine Vermittungsposition zwischen den Rechnern des internen Netzes und dem Internet ein. Wenn ein interner Rechner einen externen Server ansprechen will, so sendet er seine Daten nicht direkt dorthin, sondern statt dessen an den Proxy. Dieser kommuniziert nun im eigenen Namen mit dem externen Rechner und sendet das Ergebnis an den internen Rechner weiter. Dabei erscheint es dem externen Host so, als würde die Kommunikation vom Proxy ausgehen; die Existenz des internen Rechners wird also verschleiert. Allerdings sind nicht alle Protokolle unmittelbar für die Nutzung mit einem Proxy-Server geeignet. Teilweise ist es möglich durch geringfügige Anpassung des Benutzerverhaltens Protokolle über Proxy-Server zu nutzen, die sonst nicht dafür geeignet wären. Welche Protokolle das im einzelnen sind, wird später besprochen.

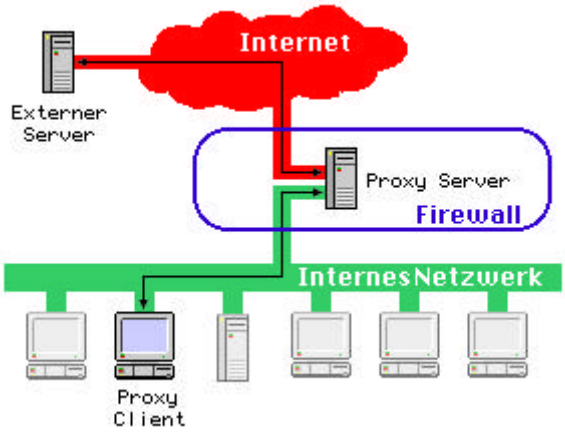

Fig.3: Nur der Proxy Server kommuniziert mit dem Internet. Alle internen Rechner arbeiten über den Proxy.

Für jeden Type von Firewall gibt es mittlerweile eine großen Zahl von Komponenten, sowohl auf dem kommerziellen als auch im Public Domain Bereich. Da aber fertige Lösungen nie alle speziellen Bedürfnisse abdecken werden, wird man beim Erstellen einer Firewall stets eine Mischung aus fertig bezogenen und selbstgeschriebenen Teilen einsetzen.

---

5. Bauformen von Firewalls:

Es gibt viele Möglichkeiten eine Firewall aufzubauen. Wer daran geht eine Firewall zu errichten kann mittlerweile zwischen einer großen Zahl von Komponenten, sowohl aus dem kommerziellen als

auch aus dem Public Domain Bereich wählen. Im folgenden sollen einige Möglichkeiten beispielhaft vorgeführt werden.

Eine technisch sehr simple Lösung setzt darauf, einen Rechner mit zwei (oder mehr) Netzanschlüssen (= Dual Homed Host) als Firewall einzusetzen. Dabei wird ein Anschluß mit dem externen Netzwerk verbunden und der (die) andere(n) mit dem internen Netz. Der Rechner kann nun alle Pakete die zwischen internem und externen Netzwerk passieren sowohl auf IP-Paket Ebene als auch auf Applikationsebene filtern. Das Problem dieser Lösung besteht darin, daß ein Rechner die einzige Verteidigung darstellt, und gleichzeitig eine relativ komplizierte (und damit fehleranfällige) Aufgabe zu erfüllen hat. Weiters werden IP-Pakete in einem Dual-Homed Host oft automatisch auf sehr tiefer Ebene des Betriebssystems geroutet, so daß es nötig ist, in das Betriebssystem einzugreifen um diese Funktion auszuschalten und einen Filter zu installieren.

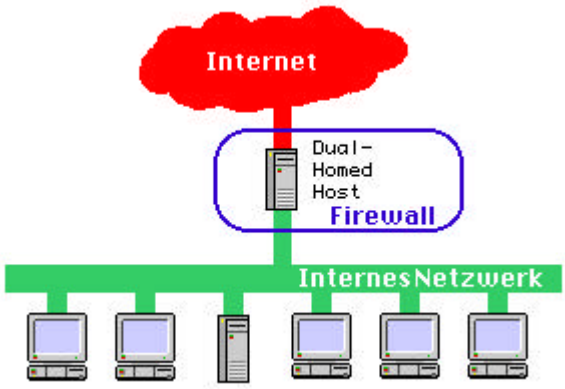

Fig.4: Eine Firewall allein aus einem Dual-Homed Host

Eine günstigere Lösung (die allerdings mehr Hardware benötigt) besteht darin die Filterung auf IP-Paket Ebene von der Applikationsebene zu trennen. Dazu wird zwischen das interne Netzwerk und das Internet ein filternder Router installiert, der verhindert daß beliebige Knoten des internen Netzes direkt Daten nach außen senden. Nur der Bollwerksrechner darf Daten über den Router mit externen Rechnern kommunizieren. Alle anderen Knoten müßen sich an ihn wenden, so daß leicht auch auf Applikationsebene gefiltert werden kann. Durch die Zweiteilung entstehen automatisch zwei Verteidigungsebenen. Damit ist auch der Bollwerksrechner selbst bereits vor Angriffen geschützt, doch sollte nie übersehen werden, daß ein Angreifer, der den Router unter seine Kontrolle gebracht hat auf dem Netzwerk (auf dem auch aller interner Datenverkehr läuft) mithören kann, ohne den Bollwerksrechner zu überwinden.

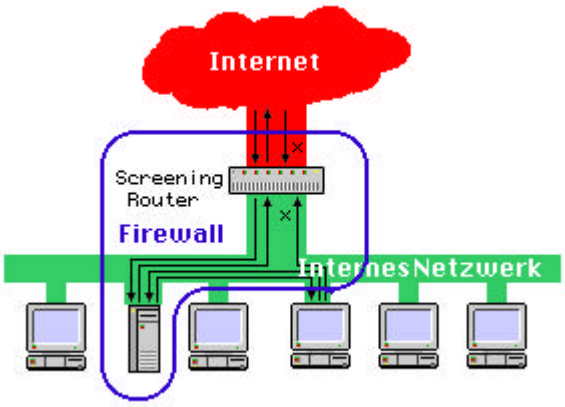

Fig.5: Beispiel einer Firewall in der Screened Host Architektur

Um eine klarere Trennung von internem und externem Datenverkehr zu erreichen kann es klug sein (unter wiederum erhöhtem Hardwareaufwand) ein eigenes peripheres Netz zu errichten auf dem nur der (oder die) Bollwerksrechner sitzen. So kann ein Eindringling, selbst wenn er den externen Router und/oder den Bastion Host in seiner Gewalt hat noch immer nicht den rein internen Verkehr

mithören.

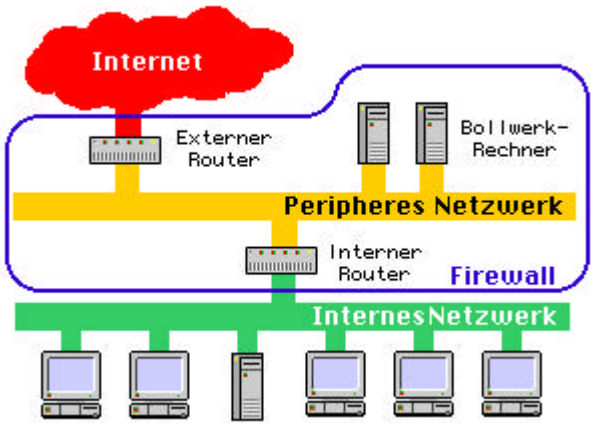

Fig.6: Beispiel einer Firewall mit einem peripheren Netzwerk

Da Router relativ sichere Geräte sind ist es auch möglich den internen und externen Router in ein Gerät zusammen zu ziehen um so den Hardwareaufwand zu vermindern. Das setzt natürlich voraus, daß der Router hinreichend flexibel ist und sowohl eingehende als auch ausgehende Pakete filtern kann. Die Filter-Regeln des Routers müssen sicherstellen, daß nie direkt Daten vom internen zum externen Netz fließen, sondern daß das periphere Netzwerk stets Quelle oder Ziel jedes Pakets ist.

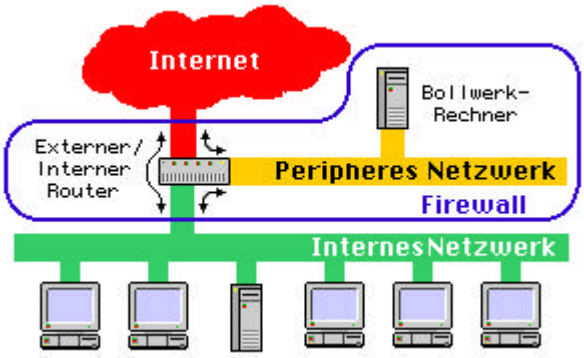

Fig.7: Es ist möglich internen und externen Router zu vereinigen.

Alternativ ist es möglich einen Dual-Homed Host als Bollwerksrechner zu verwenden und dadurch den externen Router zu sparen. Das führt zwar zu etwas größerer Verwundbarkeit des Bollwerksrechners und bringt nicht die gleiche Geschwindigkeit wie ein echter Router, doch sind die Sicherheitsverluste gering und die Datenrate im Internet wird oft mehr durch die Bandbreite des Netzzugangs als durch die Kapazität des Routers begrenzt.

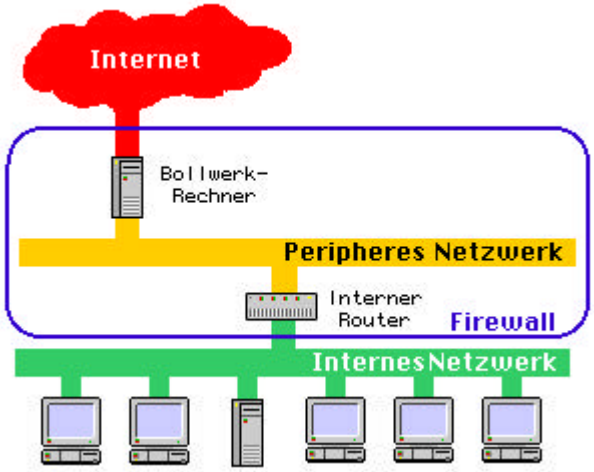

Fig.8: Es ist möglich den externer Router und den Bollwerksrechner zu vereinen.

Allerdings ist es nicht tunlich den internen Router mit dem Bollwerksrechner zu vereinen, da nun wieder alle rein internen Datenströme am Bollwerksrechner vorbeikommen und bei einer Überwindung dieses Rechners dem Angreifer offenliegen.

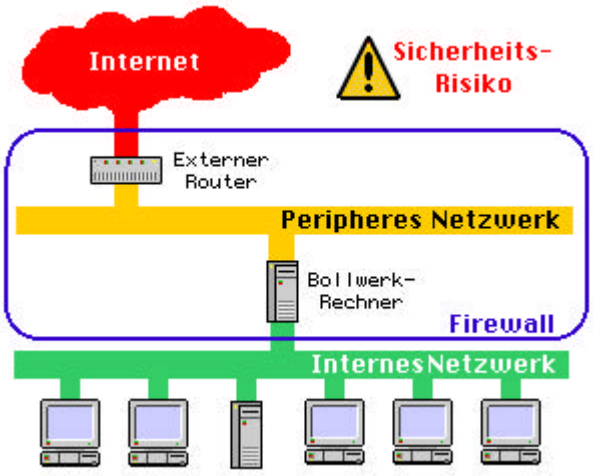

Fig.9: Es ist gefährlich den internen Router und den Bollwerksrechner zu

Auch ist es unklug (etwa zum Zweck der Durchsatzsteigerung) mehrere interne Router zu verwenden. Nun besteht die Gefahr, daß der schnellste Weg von einem internen Knoten zu einem anderen über einen internen Router auf das periphere Netzwerk und über den anderen internen Router wieder ins interne Netz führt. Somit würden rein interne Daten über das periphere Netzwerk geleitet, wo sie (vergleichsweise) einfach abgehört werden können.

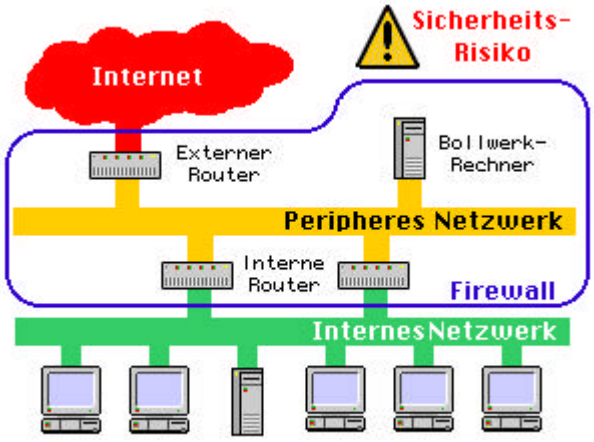

Fig.10: Es ist gefährlich mehrere interne Router zu betreiben.

Allerdings ist es durchaus möglich mehrere interne Netze an den internen Router der Firewall anzuschliessen, da die Daten bei diesem Ansatz nicht auf das periphere Netzwerk gelangen. Somit ist diese Lösung gleich sicher wie die in Fig.6 dargestellte.

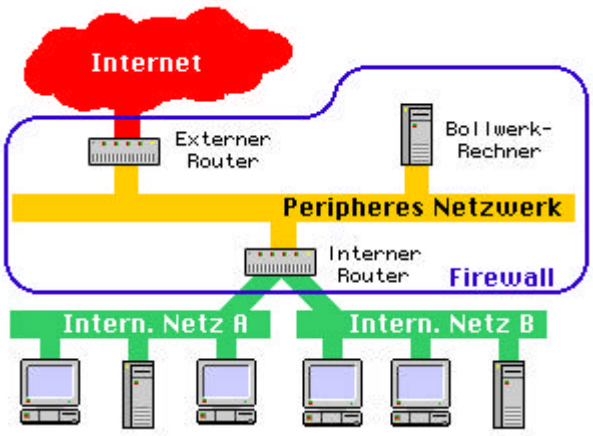

Fig.11: Es ist möglich mehrere interne Netzwerke an den interner Router einer Firewall anzuschließen.

Natürlich muß das Netzwerk hinter der Firewall nicht (wie bisher stets gezeichnet) aus einem linearen Strang bestehen. Vielmehr ist es ohne Probleme möglich beliebig komplexe Topologien hinter der Firewall einzusetzen.

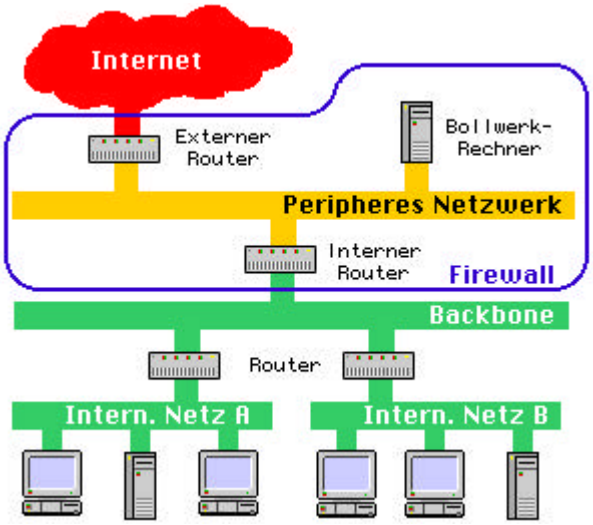

Fig.12: Es ist möglich hinter der Firewall eine komplexe Netzwerkstruktur mit mehreren Subnetzen zu verwenden.

Wenn innerhalb des internen Netzwerkes Teile mit höherem und niedrigerem Sicherheitsniveau bestehen kann auch hier eine Firewall als Trennlinie eingesetzt werden.

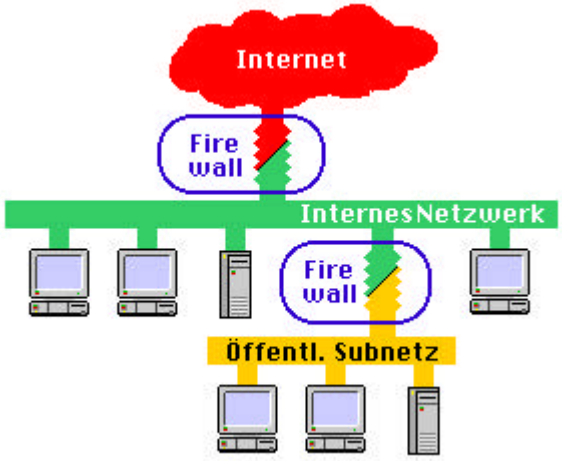

Fig.13: Unsichere Subnetze innerhalb des internen Netzwerks können mit einer internen Firewall

abgeschirmt werden.

Bücher zum Thema Firewalls:

- D.B. Chapman and E.D. Zwicky, *Building Internet Firewalls*, O'Reilly & Associates, Inc., 1995
- D.B. Chapman and E.D. Zwicky, Deutsche Übersetzung: *Internet Firewalls*, O'Reilly & Associates, Inc., 1995
- W.R. Cheswick and S.M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994
- W.R. Cheswick and S.M. Bellovin, Deutsche Übersetzung *Firewalls und Sicherheit im Internet*, Addison-Wesley, 1996
- Chris Hare and Karanjit Siyan, *Internet Firewalls and Network Security*, New Riders, 1995

Online Literatur:

- Allgemeine Documentation
  - Security with Internet Firewalls (Senior Paper)
  - Facts about Firewalls
- Link Collections:
  - Yahoo - Computers and Internet:Security_and_Encryption:Firewalls
  - Yahoo - Computers and Internet:Software:Security:Firewalls
- Firewall Producers:
  - Secure Computing Cooperation
  - Checkpoint
  - Telstra
- IPv6:
  - IPv6 (IPng) Homepage
  - CERT (Computer Emergency Respose Team) IPv6 Page
  - IPv6 für LINUX - FAQ

Zuletzt Verändert: 12. Dezember 1996
EMail: Roland LIEGER: rlieger@auto.tuwien.ac.at
EMail: Harput VAHAN: e9126197@student.tuwien.ac.at
EMail: Grzegorz RUMATOWSKI: e9425527@student.tuwien.ac.at
EMail: Patrick AWART: e9226235@student.tuwien.ac.at